PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-155834

(43)Date of publication of application : 06.06.2000

---

(51)Int.Cl. G06T 1/00
G09C 1/00
G09C 5/00
H04L 12/28
H04L 12/54
H04L 12/58
H04N 1/387

---

(21)Application number : 10-330837 (71)Applicant : CANON INC

(22)Date of filing : 20.11.1998 (72)Inventor : YOSHIDA ATSUSHI
IWAMURA KEIICHI

---

(54) ILLEGALITY DETECTING DEVICE AND ITS METHOD AND ELECTRONIC WATERMARK EMBEDDING DEVICE AND ITS METHOD AND COMPUTER READABLE STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To detect the illegality such as alteration of an electronic watermark embedded in digital contents.
SOLUTION: Digital contents in which a hash value is embedded as an electronic watermark are read from a storage device 401, and a subset to be hashed which is used

for the arithmetic operation of the hash value is extracted based on position information from the digital contents by a switch 402, and inputted to an arithmetic unit 403 so that the hash value can be obtained. On the other hand, an extracting device 404 extracts the hash value based on the position information from the digital contents. Then, the hash value obtained by the arithmetic unit 403 is compared with the extracted hash value by a comparator device 405, and when they match with each other, it is judged that the digital contents are legal, and otherwise, it is judged that the digital contents are illegal.

LEGAL STATUS [Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] A selection means to choose the plurality of the subset of the data value which constitutes the digital contents inputted, An operation means to perform a predetermined operation for every subset using the data value included in one or more predetermined subsets among two or more subsets by which selection was made [above-mentioned], A watermark extract means to extract the information currently embedded as digital watermarking from one or more of other predetermined subsets among two or more subsets by which selection was made [above-mentioned], respectively, Unjust detection equipment characterized by establishing a comparison means to compare the above-mentioned information extracted from a different subset from the subset which calculated the value calculated with the above-mentioned operation means, and this value.

[Claim 2] The above-mentioned operation means is unjust detection equipment according to claim 1 characterized by calculating the hash value of the data value included in the subset by which selection was made [above-mentioned].

[Claim 3] Unjust detection equipment according to claim 1 characterized by the location on the digital contents of two or more subsets by which selection was made [above-mentioned] continuing.

[Claim 4] Unjust detection equipment according to claim 1 characterized by including all the data values included in the above-mentioned digital contents in the subset by which selection was made [above-mentioned].

[Claim 5] Unjust detection equipment according to claim 1 characterized by including no data values included in the above-mentioned digital contents multiplex in the subset by which selection was made [above-mentioned].

[Claim 6] Unjust detection equipment according to claim 1 with which the location on the digital contents of the element which constitutes two or more subsets by which selection was made [above-mentioned] is characterized by being distributed over homogeneity at the whole digital contents.

[Claim 7] Unjust detection equipment according to claim 6 with which the above-mentioned digital contents are digital images, and the location on the digital contents of the element which constitutes two or more subsets by which selection was made [above-mentioned] is characterized by being alternately distributed on the above-mentioned digital image.

[Claim 8] Unjust detection equipment according to claim 6 with which the above-mentioned digital contents are digital images, and the location on the digital contents of the element which constitutes two or more subsets by which selection was made [above-mentioned] is characterized by being distributed in the shape of stripes on the above-mentioned digital image.

[Claim 9] Unjust detection equipment according to claim 6 with which the above-mentioned digital contents are digital images, and the location on the digital contents of the element which constitutes two or more subsets by which selection was made [above-mentioned] is characterized by being distributed in the shape of a grid on the above-mentioned digital image.

[Claim 10] Unjust detection equipment according to claim 1 with which the subset by which selection was made [above-mentioned] is characterized by being an object on digital contents.

[Claim 11] Unjust detection equipment according to claim 1 characterized by establishing a location extract means to extract the embedding positional information currently embedded as digital watermarking at the position on the above-mentioned digital contents, and the above-mentioned selection means choosing two or more subsets from the subset on the digital contents which carried out [above-mentioned] the extract, and which embed and are shown in positional information.

[Claim 12] A selection means to choose the plurality of the subset of the data value which constitutes digital contents, An operation means to perform a predetermined operation for every subset using the data value included in one or more predetermined subsets among two or more subsets by which selection was made [above-mentioned], Digital-watermarking embedding equipment characterized by establishing the embedding means which embeds the value for which the above-mentioned operation means calculated and asked one or more of other predetermined subsets from other subsets among the subsets by which selection was made [above-mentioned] as digital watermarking.

[Claim 13] The above-mentioned operation means is digital-watermarking embedding equipment according to claim 12 characterized by calculating the hash value of the

data value of the subset by which selection selection was made [above-mentioned].
[Claim 14] Digital-watermarking embedding equipment according to claim 12 characterized by the location on the digital contents of the subset by which selection was made [above-mentioned] continuing.
[Claim 15] Digital-watermarking embedding equipment according to claim 12 characterized by including all the data values included in the above-mentioned digital contents in the subset by which selection was made [above-mentioned].
[Claim 16] Digital-watermarking embedding equipment according to claim 12 characterized by including no data values included in the above-mentioned digital contents multiplex in the subset by which selection was made [above-mentioned].
[Claim 17] Digital-watermarking embedding equipment according to claim 12 with which the location on the digital contents of the element which constitutes two or more subsets by which selection was made [above-mentioned] is characterized by being distributed over homogeneity at the whole digital contents.
[Claim 18] Digital-watermarking embedding equipment according to claim 17 with which the above-mentioned digital contents are digital images, and the location on the digital contents of the element which constitutes two or more subsets by which selection was made [above-mentioned] is characterized by being alternately distributed on the above-mentioned digital image.
[Claim 19] Digital-watermarking embedding equipment according to claim 17 with which the above-mentioned digital contents are digital images, and the location on the digital contents of the element which constitutes two or more subsets by which selection was made [above-mentioned] is characterized by being distributed in the shape of stripes on the above-mentioned digital image.
[Claim 20] Digital-watermarking embedding equipment according to claim 17 with which the above-mentioned digital contents are digital images, and the location on the digital contents of the element which constitutes two or more subsets by which selection was made [above-mentioned] is characterized by being distributed in the shape of a grid on the above-mentioned digital image.
[Claim 21] Digital-watermarking embedding equipment according to claim 12 with which the subset by which selection was made [above-mentioned] is characterized by being an object on digital contents.
[Claim 22] Digital-watermarking embedding equipment according to claim 12 characterized by establishing a means for the positional information embedding which embeds the positional information which shows the location of two or more subsets by which selection was made [above-mentioned] at the position on the

above-mentioned digital contents.

[Claim 23] The procedure which chooses the plurality of the subset of the data value which constitutes the digital contents inputted, The procedure of calculating a hash value for every subset using the data value included in one or more predetermined subsets among two or more subsets by which selection was made [above-mentioned], The procedure of extracting the digital-watermarking information currently embedded as a hash value from one or more of other predetermined subsets among two or more subsets by which selection was made [above-mentioned], respectively, The unjust detection approach characterized by forming the procedure which compares the above-mentioned digital-watermarking information extracted from a different subset from the subset which calculated the hash value calculated with the above-mentioned operation procedure, and this hash value.

[Claim 24] The procedure which chooses the plurality of the subset of the data value which constitutes digital contents, The procedure of calculating a hash value for every subset using the data value included in one or more predetermined subsets among two or more subsets by which selection was made [above-mentioned], The digital-watermarking embedding approach characterized by forming the procedure which embeds the hash value for which one or more of other predetermined subsets were asked by the above-mentioned operation from other subsets among the subsets by which selection was made [above-mentioned] as digital watermarking.

[Claim 25] The processing which chooses the plurality of the subset of the data value which constitutes the digital contents inputted, The processing which calculates a hash value for every subset using the data value included in one or more predetermined subsets among two or more subsets by which selection was made [above-mentioned], The processing which extracts the digital-watermarking information currently embedded as a hash value from one or more of other predetermined subsets among two or more subsets by which selection was made [above-mentioned], respectively, The storage which memorized the program for performing processing which compares the above-mentioned digital-watermarking information extracted from a different subset from the subset which calculated the hash value calculated by the above-mentioned operation, and this hash value and in which computer reading is possible.

[Claim 26] The processing which chooses the plurality of the subset of the data value which constitutes digital contents, The processing which calculates a hash value for every subset using the data value included in one or more predetermined subsets

among two or more subsets by which selection was made [above-mentioned], The storage which memorized the program for performing processing which embeds the hash value for which one or more of other predetermined subsets were asked by the above-mentioned operation from other subsets among the subsets by which selection was made [above-mentioned] as digital watermarking and in which computer reading is possible.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the storage which is used for the digital-watermarking embedding equipment, the approach, and them which embed the unjust detection equipment which detects injustice, such as an alteration to the digital contents to which digital watermarking was embedded, an approach, and digital watermarking and in which computer reading is possible.

[0002]

[Description of the Prior Art] As compared with the conventional analog information, it can copy, and can alter in digital information, without deteriorating simply by computer etc., and there is the description that transmitting through a communication line is easy in it. According to such a description, digital information suited the inclination which is copied illegally easily and redistributed.

[0003] There is technique called digital watermarking as one of the approaches for preventing this. Digital watermarking is the technique of embedding information to human being in the form which cannot be perceived, when the digital contents currently embedded in it are reproduced to usual. In addition, in the following explanation, digital contents shall point out a dynamic image, a static image, voice, a computer program, computer data, etc.

[0004] If it says by the digital image, the technique of calculating to the data value of the digital contents which hit the hue of a pixel, lightness, etc., and embedding digital watermarking is one of typical things of the information embedding method by digital watermarking. Digital contents are divided into a block and the technique of Digimarc of spacing and adding a pattern, and a U.S. Pat. No. 5,636,292 number which is the combination of +1 and −1 and which was decided beforehand is one of typical things of this technique for every block.

[0005] As a typical thing of other digital-watermarking embedding approaches, frequency conversion, such as a fast Fourier transform, a discrete cosine transform, and wavelet transform, is performed to digital contents, and after spacing through a frequency domain and adding information, the technique of performing embedding is mentioned by performing reverse frequency conversion.

[0006] By the technique by the fast Fourier transform, after input contents added and diffuse PN sequence, they are divided into a block. And the Fourier transform is performed for every block and 1-bit watermark information is embedded at 1 block. An inverse Fourier transform is given and, as for the block with which watermark information was embedded, the contents where the again same PN sequence as the beginning was added, and digital watermarking was embedded are obtained. This technique is detailed to "Onishi, **, Matsui, and "watermark signing method to image by PN sequence" 1997, a code, information security symposium lecture collected works, and SCIS97-26B."

[0007] The technique by the discrete cosine transform is divided into a block, and carries out a discrete cosine transform for every block. After embedding 1-bit information at 1 block, inverse transformation is carried out and digital-watermarking embedding finishing contents are generated. This technique is detailed to "Nakamura, brook, and Takashima "digital-watermarking method in frequency domain for protection of copyrights of digital image" 1997, a code, information security symposium lecture collected works, and SCIS97-26A."

[0008] The technique by wavelet transform is technique to twist the need of carrying out block division of the input contents, and is detailed to "Ishizuka, Sakai, Sakurai,

and "experimental consideration about safety and dependability of electronic watermark technique using wavelet transform" 1997, a code, information security symposium lecture collected works, and SCIS97-26D."

[0009] By the above approaches, copyright information and User Information are mentioned as a typical thing of the information embedded as digital watermarking to digital contents. By embedding copyright information, as for a user, copyright's being set as digital contents and an author can know who it is. However, whether copyright is protected actually had started a user's morals. Moreover, the user who redistributed is detectable from the digital contents redistributed unjustly by embedding User Information. However, only effectiveness of extent which emits warning to a user also in this case can be desired.

[0010] It is predicted that infrastructures, such as the Internet, are further ready, network society takes for progressing, and the opportunity for digital contents to be distributed on a network will increase by leaps and bounds from now on. It is a problem about protection of copyrights to become more serious in connection with it, and it is thought that it becomes general that digital watermarking is embedded to all the digital contents also containing the digital contents to which copyright is not set depending on the case for solution of this problem.

[0011]

[Problem(s) to be Solved by the Invention] However, whether as mentioned above, for protection of copyrights, when digital watermarking is embedded by the conventional method, copyright is kept started a user's consciousness, and it had the problem that copyright could not be protected physically.

[0012] This invention was accomplished in order to solve the above-mentioned problem, and it aims at enabling it to detect the injustice over digital contents, and to embed inaccurate digital watermarking which is hard to be performed to digital contents.

[0013]

[Means for Solving the Problem] In unjust detection equipment according to this invention in order to attain the above-mentioned object A selection means to choose the plurality of the subset of the data value which constitutes the digital contents inputted, An operation means to perform a predetermined operation for every subset using the data value included in one or more predetermined subsets among two or more subsets by which selection was made [above-mentioned], A watermark extract means to extract the information currently embedded as digital watermarking from one or more of other predetermined subsets among two or more subsets by which

selection was made [above-mentioned], respectively, A comparison means to compare the above-mentioned information extracted from a different subset from the subset which calculated the value calculated with the above-mentioned operation means and this value is established.

[0014] Moreover, it sets to the digital-watermarking embedding equipment by this invention. A selection means to choose the plurality of the subset of the data value which constitutes digital contents, An operation means to perform a predetermined operation for every subset using the data value included in one or more predetermined subsets among two or more subsets by which selection was made [above-mentioned], The embedding means which embeds the value for which the above-mentioned operation means calculated and asked one or more of other predetermined subsets from other subsets among the subsets by which selection was made [above-mentioned] as digital watermarking is established.

[0015] Moreover, it sets to the unjust detection approach by this invention. The procedure which chooses the plurality of the subset of the data value which constitutes the digital contents inputted, The procedure of calculating a hash value for every subset using the data value included in one or more predetermined subsets among two or more subsets by which selection was made [above-mentioned], The procedure of extracting the digital-watermarking information currently embedded as a hash value from one or more of other predetermined subsets among two or more subsets by which selection was made [above-mentioned], respectively, The procedure which compares the above-mentioned digital-watermarking information extracted from a different subset from the subset which calculated the hash value calculated by the above-mentioned operation and this hash value is formed.

[0016] Moreover, it sets to the digital-watermarking embedding approach by this invention. The procedure which chooses the plurality of the subset of the data value which constitutes digital contents, The procedure of calculating a hash value for every subset using the data value included in one or more predetermined subsets among two or more subsets by which selection was made [above-mentioned], The procedure which embeds the hash value for which one or more of other predetermined subsets were asked by the above-mentioned operation from other subsets among the subsets by which selection was made [above-mentioned] as digital watermarking is formed.

[0017] Moreover, the processing which chooses the plurality of the subset of the data value which constitutes the digital contents inputted in the storage by this invention, The processing which calculates a hash value for every subset using the data value

included in one or more predetermined subsets among two or more subsets by which selection was made [above-mentioned], The processing which extracts the digital-watermarking information currently embedded as a hash value from one or more of other predetermined subsets among two or more subsets by which selection was made [above-mentioned], respectively, The program for performing processing which compares the above-mentioned digital-watermarking information extracted from a different subset from the subset which calculated the hash value calculated by the above-mentioned operation and this hash value is memorized.

[0018] Furthermore, it sets to other storages by this invention. The processing which chooses the plurality of the subset of the data value which constitutes digital contents, The processing which calculates a hash value for every subset using the data value included in one or more predetermined subsets among two or more subsets by which selection was made [above-mentioned], The program for performing processing which embeds the hash value for which one or more of other predetermined subsets were asked by the above-mentioned operation from other subsets among the subsets of the data value by which selection was made [above-mentioned] as digital watermarking is memorized.

[0019]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained with a drawing. Drawing 1 is drawing showing the configuration of a general network, and shows an example of the operating environment of this invention. The Internet is mentioned as a typical thing of a public network 101. The distribution server 102 and the police engine 103 which sell various digital contents represented by the digital image, and distribute, the user 104, and the Local Area Network (LAN) 105 grade are connected to the public network 101.

[0020] The distribution server 102 is World. Wide Being constituted by the Web server (Web server) is common. Moreover, LAN105 is intercepted by the fire wall 106 from the outside, and only the communication link with parameters set up beforehand, such as a class of a transmitting person and transmit data, is permitted between the LAN105 1 public networks 101.

[0021] Moreover, the printer 113 grade by which direct continuation was carried out to the display 112 connected to the display 109 connected to a proxy server 107 and a personal computer (PC)108 and PC108, a printer 110 and other PCs111, and other PCs111 and LAN105 exists in the LAN105 interior. Control at the time of PCs 108 and 111 of the LAN101 interior accessing pro KISHISA 1 BA 107 at the Web server of distribution server 102 grade is performed, and all the data that communicate among

both pass a proxy server 107.

[0022] Drawing 2 is drawing in which the protection-of-copyrights method by the gestalt of this operation was carried and in which coming proxy server 107 and showing an example. This system The bus 201 used for the data exchange between the equipment in a system, unjust detection equipment 202, the processing unit 203 which operates according to the detection result of unjust detection equipment 202, I/O Port 204, the controller 205 which controls each equipment, It consists of the external storage 208 and the display 209 which were connected to the memory 206 which saves temporarily the digital contents inputted into the system, the communication link port 207 connected with the network of the LAN105 grade system exterior, and I/O Port 204.

[0023] Unjust detection equipment 202 detects that detected the digital-watermarking information embedded to day SHITARU contents, and unjust processing was beforehand performed to these digital contents by digital-watermarking embedding equipment. When the above-mentioned digital-watermarking embedding equipment is carried in picture input devices, such as a digital camera and a scanner, it becomes detectable with unjust detection equipment 202 that injustice was performed to the digital contents inputted by this picture input device.

[0024] Moreover, it is the computer and application software with which digital-watermarking embedding equipment was carried, and the injustice over the created digital contents can be detected with unjust detection equipment 202 by creating digital contents. Moreover, digital-watermarking embedding equipment may be carried in a store, a distribution server, a network device, etc.

[0025] In this system, the digital contents used as the object for examination are read by the communication link port 207 through LAN105 and/or LAN105, and public network 101 grade. The read digital contents are temporarily saved in memory 206. The digital contents on memory 206 are inputted into unjust detection equipment 202, and it is judged whether it is just. When judged with digital contents being just with unjust detection equipment 202, it distributes to the entity which performed the distribution request of digital contents by the communication link port 207.

[0026] Moreover, when judged with digital contents being inaccurate with unjust detection equipment 202, the following any one or two or more processings are performed by the processing unit 203.

- Output to visible / entity which performed the distribution request of digital contents with the communication device 207 after performing data processing which

embeds invisible digital watermarking, such as adding filtering, encryption, a scramble, and a noise to digital contents with a processing unit 203.

[0027] - Data BESUHE writing **** which exists in the distribution server 102 and police engine 103 grade with a processing unit 203 via the external storage 208 by which the information about digital contents was connected to I/O Port 204, such as information on the acquisition origin which received digital contents, information on the entity which performed reading, and/or a name of digital contents, and/or the communication link port 207.

[0028] - Control by the controller 204 stops an output.

- A warning message is generated by the processing unit 203 and warning is displayed on the display 209 grade connected to I/O Port 204 by it. Moreover, the system by which warning is emitted by the communication link port 207 to an independent organization the acquisition origin of digital contents through NETTOWA 1 KU can also be constituted easily.

[0029] Next, the unjust detection approach used with unjust detection equipment 202 is explained. Since the approach by the gestalt of this operation is the technique of having used the hash value, a hash value is explained first. Hash value h is the short output h which is the compression value of the long input train X searched for by Hash Function f:x->h. Moreover, on the other hand, it is a tropism function, and has the property in which it is difficult to ask for a different input x which fills f(x') =f (x), and x'. MD5 (Message Digest5), SHA (Secure Hash Algorithm), etc. are one of typical things of a Hash Function. About the detail of a Hash Function, it is detailed in Eiji Okamoto work "a guide to code theoretical" (KYORITSU SHUPPAN Co., Ltd.).

[0030] The subset for a hash and the subset for embedding are first extracted from digital contents. Next, the hash value of the data value of the subset for a hash is calculated. When the data value of the subset for a hash is changed, it stops being in agreement with the calculated hash value. Since it saves without separating the calculated hash value with digital contents, it embeds as digital watermarking, and embeds and saves at an object subset.

[0031] Therefore, in the case of unjust detection, a hash value is calculated from the subset for a hash, the hash value currently embedded as digital watermarking from the subset for embedding is extracted, and the calculated hash value is compared with the extracted hash value, and when in agreement, it judges with it being just. By the unjust detection method by this invention, when the subset for a hash is altered, and when the subset for embedding is altered by extent which digital watermarking cannot extract normally, it is detected as inaccurate.

[0032] In order to raise detection precision more, it is possible to arrange by turns the data value which embeds with the data value belonging to the subset for a hash, and belongs to an object subset. It may take to alternate ** in units, such as a case where shall treat a digital image as digital contents, embed with the pixel of the subset for a hash as an example, and the pixel of an object subset is taken by turns per bit string of a raster (horizontal bit string) unit or length on digital contents, and a rectangle on a bit, a bit string, or digital contents. Under the present circumstances, if it embeds with the subset for a hash and the sum of an object subset is in agreement with the whole digital contents, the alteration about the whole digital contents will be detected.

[0033] Moreover, it is detectable by performing only a partial alteration as follows. That is, per the object on digital contents, or part, a hash value is calculated and an alteration in an object unit and a partial unit is also detected by embedding the calculated hash value into other objects or parts.

[0034] Next, the gestalt of operation at the time of constituting unjust detection equipment 202 and digital-watermarking embedding equipment from hardware is explained. In addition, unjust detection equipment and digital-watermarking embedding equipment are easily realizable besides a hardware configuration with the computer system configuration by software.

[0035] Drawing 3 is the block diagram showing the gestalt of operation of the 1st of digital-watermarking embedding equipment. The input to this equipment is positional information expressed with the set of digital contents and a coordinate value etc. This equipment receives control by the store 301 and the inputted positional information, and consists of embedding equipment 304 which makes digital watermarking the arithmetic unit 303 which calculates a hash value from the data value of the subset for a hash of the digital contents divided into 302 or 2 switches which extract the data value of the subset for a hash from digital contents, and the calculated hash value, and embeds it into the 2nd part of the divided digital contents. Positional information is information expressed in the coordinate location where a watermark is embedded etc. here.

[0036] The data value of the inputted digital contents is temporarily memorized by storage 301, in order to adjust a time gap. The data value memorized by the store 301 is inputted into a switch 302, and the subset for a hash which has a hash value calculated by positional information is extracted. The subset for a hash is inputted into an arithmetic unit 303. The hash value obtained as a count result of an arithmetic unit 303 is inputted into embedding equipment 304, and is embedded as digital watermarking to the digital contents saved at the store 301.

[0037] Under the present circumstances, the embedding of digital watermarking receives control by positional information, and the object which embeds digital watermarking serves as a data value in the subset for embedding. Moreover, since the subset for embedding does not cross the subset for a hash, the hash value calculated from the data value included in the subset for a hash of digital contents does not change by embedding digital watermarking.

[0038] Drawing 4 is the block diagram showing the gestalt of operation of the 1st of unjust detection equipment. The input to this equipment is the positional information same with having inputted into the digital contents for examination, and the digital-watermarking embedding equipment of drawing 3 . This equipment from the data value of the store 401 which adjusts a time gap, and the digital contents which received control by positional information and were inputted By the same approach as the switch 401 and drawing 3 which extract the subset for a hash where digital watermarking is not embedded From the arithmetic unit 403 and digital contents which calculate a hash value from the data value included in the subset for a hash of digital contents, as digital watermarking It consists of comparison equipment 405 which compares the digital-watermarking extractor 404 which extracts the hash value currently embedded, and the hash value calculated from the subset for a hash with the hash value extracted from digital contents.

[0039] The digital contents for [which was inputted into this equipment] examination are first memorized by storage 401 temporarily. The digital contents saved at the store 401 are inputted into a switch 401, and extract the subset for a hash used for the operation of a hash value from digital contents by the same positional information as drawing 3 . The subset for a hash is inputted into an arithmetic unit 403, and a hash value is calculated. Moreover, the digital contents memorized by the store 401 are inputted into the digital-watermarking extractor 404 with positional information, and the hash value currently embedded to digital contents is extracted.

[0040] When it is inputted into comparison equipment 405, is compared and is in agreement, the hash value calculated by the arithmetic unit 403 and the hash value extracted by the digital-watermarking extractor 404 output that digital contents are just, and when not in agreement, it outputs that digital information contents are unjust.

[0041] Drawing 5 is the block diagram showing the gestalt of operation of the 2nd of digital-watermarking embedding equipment. This equipment consists of digital-watermarking embedding equipment 506 which embeds to digital contents by making the switch 503 which extracts the data value included in the subset for a hash detected by the field detection equipment 502 which extracts the subset for a hash,

and the subset for embedding with field detection means, such as binary-izing, and field detection equipment 502 from a store 501 and the digital contents which were inputted, the arithmetic unit 504 which calculate a hash value from the extracted data value, and the hash value which were calculated into digital watermarking.

[0042] The inputted data value is memorized by storage 501. From a store 501, field detection equipment 502 reads a data value, and detects an object domain by approaches, such as binary-izing. The coordinate information for determining an object domain etc. may be inputted into field detection equipment 502. The digital contents memorized by the store 501 are inputted into a switch 503, and the data value included in the subset for a hash extracted by field detection equipment 502 is extracted.

[0043] The extracted data value is inputted into an arithmetic unit 504. The hash value obtained as a count result of an arithmetic unit 504 receives control of field detection equipment 502, is inputted into embedding equipment 505 and embedded as digital watermarking at the subset for embedding of the digital contents saved at the store 501.

[0044] Drawing 6 is the block diagram showing the gestalt of operation of the 2nd of unjust detection equipment. The inputs to this equipment are the digital contents for examination. This equipment With field detection means, such as binary-izing, from a store 601 and the inputted digital contents With the field detection equipment 602 and the field detection equipment 602 which extract the subset for a hash, and the subset for embedding From the subset for embedding of the switch 603 which describes the data value included in the extracted subset for a hash, the arithmetic unit 604 which calculates a hash value from the extracted data value, and digital contents It consists of comparison equipment 606 which compares the hash value calculated by the digital-watermarking extractor 605 which extracts the hash value currently embedded as digital watermarking, and the arithmetic unit 604 with the hash value extracted by the extractor 605.

[0045] The digital contents for [which was inputted into this equipment] examination are memorized by storage 601. Field detection equipment 602 considers the digital contents memorized by the store 601 as an input, and extracts the same subset for a hash as the field detection equipment 502 of drawing 5 , and the subset for embedding with means, such as binary-izing. Coordinate information for field detection equipment 602 to determine an object subset etc. may be inputted. The data value of the digital contents memorized by the store 601 is inputted into a switch 603 with the output of field detection equipment 602, and the data value included in the subset for a hash is

extracted.

[0046] The extracted data value is inputted into an arithmetic unit 604, and a hash value is calculated. Moreover, the digital contents memorized by the store 601 receive control of field detection equipment 602, it is inputted into the extractor 604 which extracts the information currently embedded as digital watermarking, and the hash value currently embedded is extracted. When the hash value calculated by the arithmetic unit 604 and the hash value extracted by the extractor 605 are compared by comparison equipment 606 and is in agreement, it outputs that digital contents are just, and when not in agreement, it outputs that digital contents are unjust.

[0047] Drawing 7 is the block diagram showing the gestalt of operation of the 3rd of digital-watermarking embedding equipment. This equipment With field detection means, such as binary-izing, from a store 701 and the inputted digital contents With field detection equipment 702 from the field detection equipment 702 and digital contents which extract the subset for a hash, and the subset for embedding The switch 703 which extracts the data value included in the detected subset for a hash, the arithmetic unit 704 which calculates a hash value from the extracted data value, and the calculated hash value are made into digital watermarking. It consists of embedding equipment 706 which embeds the positional information of the field detected by the digital-watermarking embedding equipment 705 embedded to digital contents, and field detection equipment 702 at the position of digital contents.

[0048] The inputted data value is memorized by storage 701. Field detection equipment 702 reads a data value from a store 701, and detects the object domain which exists in the field which does not overlap the position shown by embedding positional information by approaches, such as binary-izing. The coordinate information for determining an object domain etc. may be inputted into field detection equipment 702. The digital contents memorized by the store 701 are inputted into a switch 703, and the data value included in the subset for a hash extracted by field detection equipment 702 is extracted.

[0049] The extracted data value is inputted into an arithmetic unit 704. The hash value obtained as a count result of an arithmetic unit 704 receives control of field detection equipment 702, is inputted into embedding equipment 705 and embedded as digital watermarking at the subset for embedding of the digital contents saved at the store 701. The digital contents where digital watermarking was embedded embed, are inputted into equipment 706 and embedded with positional information, such as a coordinate value which can specify the subset for embedding as the position according to the embedding positional information which shows the location which

does not overlap the subset for embedding, and the subset for a hash, the same positional information of the subset for a hash, etc.

[0050] Drawing 8 is the block diagram of unjust detection equipment showing the gestalt of the 3rd operation further. The input to this equipment is the digital contents and embedding positional information for examination. This equipment from a store 801 and the inputted digital contents The positional information of the subset for a hash currently embedded as digital watermarking, From and the digital-watermarking extractor 802 and digital contents which extract the positional information of the subset for embedding From the subset for embedding of the switch 803 which extracts the data value included in the subset for a hash extracted by field detection equipment 802, the arithmetic unit 804 which calculates a hash value from the extracted data value, and digital contents It consists of comparison equipment 806 which compares the hash value calculated by the digital-watermarking extractor 805 which extracts the hash value currently embedded as digital watermarking, and the arithmetic unit 804 with the hash value extracted by the extractor 805.

[0051] The digital contents for [which was inputted into this equipment] examination are memorized by storage 801. An extractor 802 considers the digital contents memorized by the store 801 as an input, and specifies the subset for a hash, and the subset for embedding from the positional information currently embedded as digital watermarking at the position. The data value of the digital contents memorized by the store 801 is inputted into the switch 803 which receives control of field detection equipment 802, and the data value included in the subset for a hash is extracted.

[0052] The extracted data value is inputted into an arithmetic unit 804, and a hash value is calculated. Moreover, the digital contents memorized by the store 801 are inputted into the extractor 804 which receives control of field detection equipment 802, and the hash value which embeds as digital watermarking and is embedded at the object subset is extracted. The hash value calculated by the arithmetic unit 804 and the hash value extracted by the extractor 805 output that digital contents are just, when it is compared by comparison equipment 806 and is in agreement, and when not in agreement, it outputs that digital contents are unjust.

[0053] Next, the storage as a gestalt of other operations of this invention is explained. Constituting from hardware can also constitute this invention from a computer system by which ****** is constituted from a CPU and memory. When it constitutes from a computer system, the above-mentioned memory constitutes the storage by this invention. That is, the object of this invention can be attained by using the storage which memorized the program code of the software for performing actuation

explained with the gestalt of operation mentioned above with a system or equipment, and reading and performing the program code with which CPU of the system and equipment was stored in the above-mentioned storage.

[0054] Moreover, as this storage, semiconductor memory, such as ROM and RAM, an optical disk, a magneto-optic disk, a magnetic medium, etc. may be used, and these may be constituted and used for CD-ROM, a floppy disk, a magnetic medium, a magnetic card, a non-volatile memory card, etc.

[0055] Therefore, while a function equivalent to the gestalt of the above-mentioned implementation is realizable also by using with the alien systems and equipment other than the system which showed this storage to drawing 2 - drawing 8 , or equipment, and reading and performing the program code with which that system or computer was stored in this storage, equivalent effectiveness can be acquired and the object of this invention can be attained.

[0056] Moreover, when OS which is working on a computer performs a part or all of processing, Or after the program code by which reading appearance was carried out from the storage was written in the memory with which the extension unit connected to the extension board inserted in the computer or the computer is equipped, Also when CPU with which the above-mentioned extension board and an extension unit are equipped performs a part or all of processing based on directions of the program code, while being able to realize a function equivalent to the gestalt of the above-mentioned implementation, equivalent effectiveness can be acquired and the object of this invention can be attained.

[0057]

[Effect of the Invention] As explained above, while being able to add the noise or being able to detect that injustice, such as an attack of an alteration or image transformation, was made by intentionally to digital watermarking by embedding values, such as a hash value calculated from the subset of digital contents, at digital watermarking according to this invention, when injustice was detected, protection of copyrights, such as changing digital contents into the condition of not being suitable for an activity, became possible.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is structure-of-a-system drawing which consists of a device connected with the general public network which can apply this invention, and a public network.

[Drawing 2] It is the block diagram showing the example of loading of cis- TEMUHE of the protection-of-copyrights method of this invention.

[Drawing 3] It is the block diagram showing the gestalt of operation of the 1st of the digital-watermarking embedding equipment by this invention.

[Drawing 4] It is the block diagram showing the gestalt of operation of the 1st of the unjust detection equipment by this invention.

[Drawing 5] It is the block diagram showing the gestalt of operation of the 2nd of the digital-watermarking embedding equipment by this invention.

[Drawing 6] It is the block diagram showing the gestalt of operation of the 2nd of the unjust detection equipment by this invention.

[Drawing 7] It is the block diagram showing the gestalt of operation of the 3rd of the digital-watermarking embedding equipment by this invention.

[Drawing 8] It is the block diagram showing the gestalt of operation of the 3rd of the unjust detection equipment by this invention.

[Description of Notations]

202 Unjust Detection Equipment

203 Processing Unit

205 Controller

301, 501, 701 Storage

302, 503, 703 Switch

303, 504, 704 Arithmetic unit

304, 505, 705, 706 Embedding equipment

502 702 Field detection equipment

401, 601, 801 Storage
402, 603, 803 Switch
403, 604, 804 Arithmetic unit
404, 605, 802, 805 Extractor
405, 606, 806 Comparison equipment
602 Field Detection Equipment